NEWS centre
- Latest news
- Last 7 days
- Hot topics
- News analysis
- Newsletters
- News Pocket edition
- News Wap edition
- Mole

News areas

WHERE ARE YOU?
Security /Hacking /News

Boffins fight hackers with the Therminator

By James Middleton [27-03-2002]

Networks secured with hacker tactics

Scientists at California's Naval Postgraduate School in Monterey are using hacker methodology to beat the bad guys, by incorporating automated scanning routines in a network perimeter guardian known as the Therminator.

Automated scanning agents have been employed by hackers and virus writers for some time now. They can be set up to work on their own, looking for vulnerable boxes to infiltrate and take over as 'zombies'.

Some of the most infamous examples of this technique are the summer of 2000 attacks on a host of big-name sites including eBay, Yahoo and Amazon.

But scientists at the RIDLR (Reconfigurable Intrusion Detection Laboratory Research) of the naval school think this type of automatic prowling could be tweaked to work in favour of network security.

The key is getting the Therminator, a software guardian that patrols the boundaries of a network, to report back on unusual activity.

John McEachen, assistant professor of electrical and computer engineering at the naval school, argues that the problem with current intrusion detection software (IDS) is that it notifies you after the event, when the network has already been breached, because it's based on pattern recognition.

In an interview in the *Miami Herald*, McEachen said that intrusion alerts are triggered by systems that identify known patterns of programs used for intrusion.

"The problem is that you have to have seen a pattern in the past in order to be able to detect it again and identify an attack," he said.

The developers of the Therminator reckon that hackers are getting smart about this flaw and learning to avoid repetition in their attacks. "Most of these people are clever enough to do the unusual," said McEachen. And that's just what the Therminator looks for.

Based on mathematical algorithms developed by the NSA

Search News
Go!

In the Security area today

News
- eBay fraud - the scam of the future (Hacking)
- BT slammed for ignoring 'massive security risk' (Hacking)

Analysis
- Bug-beaters seek standards (Bugs and fixes)

Features
- Viewpoint: Packets in brown paper bags (Antivirus)

Products

- APC Lapdog (Hacking)
- McAfee VirusScan Online (Antivirus)

Download
- McAfee.com Personal Firewall (Hacking)

and the Sans Institute, Therminator looks for unusual spikes in activity, or unusual traffic or packets entering the network.

During tests on the network at US Pacific Command in Hawaii, the Therminator detected a major intrusion into the network within half an hour.

Over a 15-day test, the researchers also detected a distributed attack launched from four different sites in the US and Canada by the same person.

Therminator has since been deployed at Fort Belvoir in Vancouver and Fort Huachuca, Arizona.

The only downside of the system is its requirement for huge amounts of raw processing power: the Therminator deployment at the naval school uses a $50,000 Sun blade server.

McEachen pointed out that Therminator is not a defence mechanism in itself. It was designed to be used alongside other security systems such as firewalls as a pre-emptive method of defence, not a solitary guardian.

RELATED ARTICLES

- **eBay fraud - the scam of the future** [27-03-2002]
- **High noon for hackers** [15-02-2002]
- **Bug Watch: Hacker motivation** [15-01-2002]

PRINTER VERSION

SEND TO A FRIEND

FEEDBACK

AN ORIGINAL ARTICLE FROM